SAAJ 日本システム監査人協会報

自由民主党「金融検査士制度」を検討
ーシステム監査技術者の活用を申し入れー

No. 293　荒川　幸式

自民党は「金融不正再発防止対策特別調査会(会長野呂田芳成衆議院議員)」を発足させ、金融検査制度の改革について検討を始めた。このなかで会計やコンピュータの専門家について民間からの人材登用が検討されている。

会計の専門家は公認会計士が想定されているが、コンピュータの専門家については明確でないため、3月27日に橘和会長・和貝副会長と私の3名で衆議院第二議員会館に野呂田議員を訪問し、秘書の松本吉泰氏にコンピュータの監査の専門資格者として、システム監査技術者の活用を文書で申し入れた。

松本氏は、金融業界のみならず、すべての産業でシステム監査が必要ではないかと質問されるなど積極的な姿勢で対応された。

大蔵省新検査制度に移行
大蔵省金融検査部が外部人材登用へ

No. 293　荒川　幸式

大蔵省は、これまでの金融機関に対する検査制度を大幅に改革し、新検査制度を4月1日より発足させると3月31日に発表した。これまでの検査手法は検査官による精査のみであったが、新検査制度では金融機関自身の検査部門の検査結果を活用するものに変わることとなった。

今後金融機関は、自己責任原則に基づき、検査部門や監査役・公認会計士などによる検査・監査を充実させる必要がある。大蔵省は、これらの検査機構が機能していることを前提とした検査を実施する。

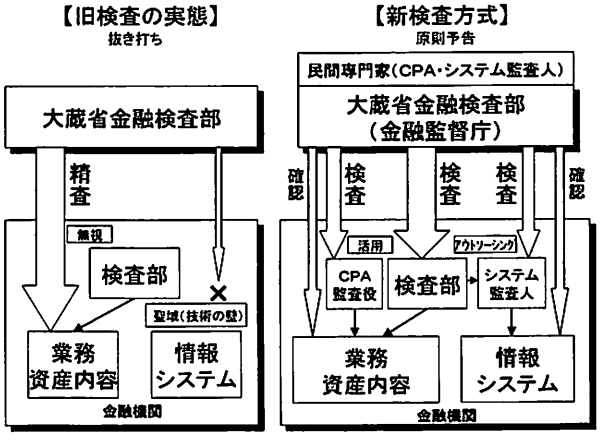
コンピュータ部門については、これまで検査部門にコンピュータの専門知識を有する要員がいないことなどを理由に、ほとんどシステム監査が行われてこなかった。これに対して大蔵省は、検査部に要員が得られない場合には、外部の専門家にアウトソーシングするように求めている。「外部の専門家」の範囲については明確にされていないが、システム監査技術者がその筆頭にあげられることは自明である。

さらに大蔵省自体の専門力の強化のため、民間の専門家の導入を図ることも同時に公表された。コンピュータの専門家についても、出向などを通じて協力を得たいとしている。

これに先立つ3月31日に、橘和会長と私が同省金融検査部を訪問し、「外部の専門家」には、システム監査技術者の活用を図るように要望した。対応された同部管理課企画官青木直幸氏と上席金融証券検査官川村健三氏は、システム監査技術者についてはご存知なかったが、金融検査におけるシステム監査の重要性について強調され、コンピュータの監査抜きには金融検査は成り立たないという認識を示された。

青木氏によれば、これからの金融検査を実効あるものとし、米国の現在の状態にまで向上させるには4000名の検査要員が必要となるとのことである。しかし、現在金融検査に関与する職員は、大蔵省(6月に発足する金融監督庁に移行する。総人数は400名)・日本銀行・財務局を合わせても800名に満たない。そこで金融機関における自主検査・監査の充実がますます重要となるとのことであった。

4月からの新検査方式による大蔵省検査をすでに受けた金融機関によれば、検査内容が大変厳しくなっているとのことであり、金融機関におけるシステム監査は急速に充実するものと思われる。



プライバシーマーク制度とシステム監査

No.223 (株)CRC総合研究所 芳仲宏

I. はじめに

個人情報の盗用、流出などの不祥事が相次いで起きているさなか、通商産業省(MITI)と日本情報処理開発協会(JIPDEC)の主催による「個人情報保護に係わる説明会」が平成10年4月17日に開催された。この説明会の内容を報告して欲しいと日本システム監査人協会(SAAJ)からの依頼があり、依頼者の話では、「資料はたくさんあるから、簡単にまとめてくれればいいのですよ。」と言われ、たまにはSAAJのお手伝いも良かろうと引き受けた次第です。天気予報ではゴールデンウィーク中の1日は雨が降る筈だとの事で、その日にちょこちょことPCに向かえば出来るだろうと考えた訳です。

説明会では、①堀部政男中央大学法学部教授(一橋大学名誉教授)から「世界の個人情報保護制度と日本」、②通商産業省機械情報産業局情報処理システム開発課藤澤秀昭企画係長から「プライバシー保護に関する国際動向と政策」、③日本情報処理開発協会情報セキュリティ対策室関本貢次長から「プライバシーマーク制度について」の講演・説明が行われた。内容全てを紹介する事は紙面の関係で出来ないが、①、②、③の講演と配付資料をベースにして記述する。

II. プライバシーについて

堀部政男中央大学法学部教授(一橋大学名誉教授)の講演からプライバシーに関する部分を要約する。[注1]

プライバシー権(right of privacy)が提唱されたのは、1890年アメリカで新聞・雑誌などのプレスが個人の私生活を取り上げるようになってきたことに対して、新たな権利を主張し、私的な事柄を法的に保護することを目指し、「一人にしておかれる権利」(right to be alone)から始まっているとの由。

日本では、三島由起夫の小説「宴のあと」によるプライバシー侵害裁判で、1964年東京地裁判決で、「私生活をみだりに公開されないという法的保障ないし権利」としてプライバシー権の必要性が論じらた。

プライバシー問題は、プレスやメディアの発達したマスメディア情報化社会における個人情報保護として、マスメディアプライバシーが、情報化社会のコンピュータ利用の拡大と共に、デジタル化した個人情報に対する保護としてコンピュータプライバシーが、更には、ネットワークの進展でネットワークプライバシーが、ネットワークのグローバル化につれて、世界ネットワークプライバシーが論じられるようになった。

プライバシー権は、当初の「一人にしておかれる権利」に加えて、「自己に関する情報の流れをコントロールする個人の権利(自己情報コントロール権)」(individual's right to control the circulation of information relating to oneself)の概念が理解されるようになってきた。

1980年には、OECD「プライバシー保護と個人データの国際流通についてのガイドラインに関する理事会勧告」(Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data)から8原則が出された。

① 収集制限の原則(Collection Limitation Principle)
個人データの収集には、制限を設けるべきであり、いかなる個人データも、適法かつ公正な手段によって、かつ適当な場合には、データ主体に知らしめ又は同意を得た上で、収集されるべきである。

② データ内容の原則(Data Quality Principle)
個人データは、その利用目的に沿ったものであるべきであり、かつ利用目的に必要な範囲内で正確、完全であり最新なものに保たれなければならない。

③ 目的明確化の原則(Purpose Specification Principle)
個人データの収集目的は、収集時より遅くない時点において明確化されなければならず、その後のデータの利用は、当該収集目的の達成又は当該収集目的に矛盾しないでかつ、目的の変更毎に明確化された他の目的の達成に限定されるべきである。

④ 利用制限の原則(Use Limitatiom Principle)
個人データは、目的明確化の原則により明確化された目的以外のために開示、利用その他

の使用に供されるべきではないが、次の場合にはこの限りではない。
(a)データ主体の同意がある場合、又は、
(b)法律の規定による場合

⑤ 安全保護の原則(Security Safeguards Principle)
データは、その紛失若しくは不当なアクセス・破壊・修正・開示の危険に対し、合理的な安全保護措置により保護されなければならない。

⑥ 公開の原則(Openness Principle)
個人データに係る開発、運用及び政策については、一般的な公開の政策が取られなければならない。個人データの存在、性質及びその主要な利用目的とともにデータ管理者の識別、通常の住所をはっきりさせるための手段が容易に利用できなければならない。

⑦ 個人参加の原則等(Individual Participation Principles)
個人はつぎの権利を有する。
(a)データ管理者が自己に関するデータを有しているか否かについて、データ管理者又はその他の者から確認を得ること。
(b)自己に関するデータを、
・ 合理的な期間内に
・ もし必要なら、過度にならない費用で、
・ 合理的な方法で、かつ
・ 自己にわかりやすい形で、自己に知らしめること。
(c)上記(a)及び(b)の要求が拒否された場合には、その理由が与えられること及びそのような拒否に対して異議を申し立てることができること。
(d)自己に関するデータに対し異議を申し立てること、及びその異議が認められた場合には、そのデータを消去、修正、完全化、補正させること。

⑧ 責任の原則(Accountability Principle)
データ管理者は、上記の諸原則を実施するための措置に従う責任を有する。

これら8原則は日本でも話題になったが、国際間のデータ流通が盛んになってきたこと等を受けて、欧州連合(EU)において1995年10月に、いわゆるEU指令「個人データ処理に係る個人情報保護及び当該データの自由な移動に関する1995年10月24日の欧州議会及び理事会の95／46／EC指令」(Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to processing of personal date and on the free movement of such date)が採択され、第三国へのデータの移転については、「当該第三国が、十分なレベルの保護(adequate level of protection)を確保している場合に限って行うことが出来る。」としている。

注1：要約にあたっては、当日配付された堀部教授の「世界の個人情報保護制度と日本」と題する資料からも抜粋させて頂いた。したがって、個人情報保護に関するOECDの8原則等の訳も同資料に拠っている。

III. プライバシーマーク制度創設について

通商産業省情報処理システム開発課藤澤秀昭企画係長から、堀部政男中央大学法学部教授(一橋大学名誉教授)の講演を受けた形で、「プライバシー保護に関する国際動向と政策」と題して講演された。ここでは、プライバシーマーク制度の創設に関する部分のみ記述する。

前述のEU指令がEU加盟各国に対して個人情報保護のために1998年(平成10年)10月までに法制化を図るよう求めた。日本はEUの加盟国ではないが、加盟各国以外(第三国)への個人情報移転は、当該第三国が十分なレベルの保護措置を講じている場合に限られるとしているため(EU指令第25条)、情報経済活動への影響が懸念されるとして、個人データ保護のため法制化が関係機関で検討され、平成9年3月4日通商産業省告示第98号として「民間部門における電子計算機処理に係る個人情報の保護に関するガイドライン」が公表され(平成元年に策定されたガイドラインの改訂)、このガイドラインの活用、周知を図るため、通商産業省は、1998年(平成10年)2月に「個人情報保護ハンドブック」を策定し、配布を開始している。注2:

今回の個人情報保護ガイドラインの改訂は、OECDガイドラインやEU指令を考慮しており、日本のプライバシーマーク制度は、EU委員会、EU加盟諸国等との話し合いで、EU指令の定める"十分なレベルの措置"に該当するものであることは確認されているとのこと。米国では、類似の仕組みとして、マークではなくシールがあるそうである。

注2:「個人情報保護ハンドブック」は、通産省情報処理システム開発課個人情報保護ガイドライン担当に請求すれば入手できる。

IV. プライバシーマーク制度について

JIPDEC情報セキュリティ対策室関本貢次長からプライバシーマーク制度の概要説明があった。ここでは、配布された資料とJIPDECのホームページ「プライバシーマーク制度の創設・運用開始について」から、「プライバシーマーク制度の骨子(抜粋)」として紹介する。注3:

1. 概　要

個人情報の取扱いについて適切な保護措置を講ずる体制を整備している民間事業者等に対し、その旨を示すマークとしてプライバシーマークを付与し、事業活動に関してプライバシーマークの使用を認容する制度。

2. 目　的

プライバシーマーク制度は、個人情報の保護に関する個人の意識の向上を図ること、民間事業者の個人情報の取扱いに関する適切性の判断の指標を個人に与えること、民間事業者に対して個人情報保護措置(コンプライアンス・プログラム、以下「C／P」という。)へのインセンティブを与えることを目的とする。

3. 実施体制

(1) 付与機関(プライバシーマーク付与機関)
財団法人日本情報処理開発協会。

(2) 指定機関(プライバシーマーク付与指定機関)
個人情報を取扱う民間事業者を会員とする事業者団体で、付与機関から指定を受けた団体。

(3) プライバシーマーク制度委員会
有識者、業界団体代表、消費者代表、法曹界代表等で構成する付与機関内の委員会。プライバシーマーク制度全般に係る事項を審議。

(4) 消費者相談窓口
付与機関内に設置。個人情報保護に係る問合せ、苦情等への対応。

4. マーク付与の対象、単位、使用できる場所

(1) 対　象
通商産業省の個人情報保護ガイドラインに準拠したC／Pを策定し、実際に個人情報の保護を推進している民間事業者

(2) 単　位
民間事業者単位(事業部、工場又は業務単位等の場合も可能)。

(3) マークを使用できる場所等
・店頭　・封筒
・契約約款　・便箋
・説明書　・名刺
・宣伝・広告用資料　・ホームページ　等

5. マーク付与の有効期限

有効期限は2年間。以降は2年毎の更新。

6. マーク付与の条件

付与認定基準に合格すること(下記は、その一例)。

付与認定基準の一例として挙げられている。

- 通産省の個人情報保護ガイドライン又は業界ガイドラインに準じたC／P(コンプライアンス・プログラム：実戦順守計画)注4:を定めていること。
- C／Pに基づいて個人情報の管理が適切に実施されていること。
- 個人情報を適切に取扱う体制が整備されていること。
- 個人情報の管理者が指名されていること。
- 企業外部への個人情報の提供、取扱いの委託を行う際には、責任分担や守秘に係る契約を締結する等、個人情報について適切な保護が講じられるよう措置されていること。
- 年1回以上、個人情報の機密保持に係わる周知徹底の措置を講じていること。
- 年1回以上、事業者内部の個人情報の保護の状況を監査すること。
- 個人情報保護に関する相談窓口が常設されていること。

注3:紹介と抜粋については、JIPDEC関係者の了解を得ている。

注4:C／Pに関する説明(配付資料からそのまま抜粋)
コンプライアンス・プログラムは、実践順守計画とも言います。これは、個人情報保護ガイドラインに準じて事業者が個人情報を適切に取扱うために定めた社内規程や指針のようなものです。
したがって、コンプライアンス・プログラムの趣旨、内容が社員等に周知徹底されていることが必要で、その上、実行可能なものであることが求められます。

V. プライバシーマーク制度と監査

プライバシーマーク制度の説明資料の中から、監査に関連する事項が幾つか出てきます。システム監査に関心を持たれる方には、知っておいて頂きたい事項を紹介します。

1. 監査の態様

プライバシーマーク制度では、「年1回以上、事業者内部の個人情報の保護の状況を監査すること。」がマーク付与の条件の一つになっている。

この監査は、プライバシーマーク制度創設に至る背景説明を聞いている限りでは、電子化された個人情報データを監査対象とせざるを得ないことを考えると、システム監査の事を指していると思ったが、念のため、説明会席上で質問したところ、「マーク付与申請企業によっては、監査の実施体制や形態が種々異なるので、監査と表現した。監査にはシステム監査も含まれる。」旨の回答があった。事実、プロジェクターの画面には、監査の例として「システム監査」の文字が踊っていた。

私見：したがって、システム監査人としては、今後、プライバシーマーク制度におけるシステム監査のあり方とその対応につき留意しなければならないだろう。システム監査基準には、留意事項として、監査実施に際して活用すべき指針が記載されており、通産省のシステム監査基準、情報システム安全対策基準、コンピュータウイルス対策基準、コンピュータ不正アクセス対策基準、ソフトウェア管理ガイドライン、警察庁の情報システム安全対策指針に加えて、通産省の「個人情報保護ガイドライン」も付加した方が良いだろう。

2. 監査体制と回数

プライバシーマーク付与申請書には、「個人情報の保護に係わる監査と年間の監査回数」を記載する欄があり、説明資料では次の様式で記載することになっている。

(1) 監査の体制
　監査の実施主体(内部監査部門、外部の監査企業)、監査結果の報告先
　内部監査部門の場合は、人数と経験年数を明記

(2) 監査に関する規定等
　(規定の概要、制定又は改訂年月日)

(3) 年間の監査回数

私見：プライバシーマーク使用を認定された企業が情報サービス会社で、通産省の安全対策実施事業所認定企業や、SO認定企業である時、それぞれの制度のなかで、年1回以上、目的に応じてシステム監査を実施する事が義務づけられている。これらのシステム監査では、監査テーマによっては、当然の事ながら、データ保護、データセキュリティの面からプライバシー保護に関する監査も重要な監査ポイントである。この様な場合、プライバシーマーク制度で言うところの「個人情報の保護の状況を監査すること。」という付与の条件に合致すると理解して良いのか、あるいは、別途、プライバシーマーク制度に対応する為だけの監査をしなければならないのかは、未だ関係者に確認していない。プライバシーマーク制度の趣旨から考えれば、これらの監査も回数としてカウントし、色々な視点からシステム監査を実施することにより個人情報の保護を図ることが大切と考える。

3. 監査報告

配布された資料の中に、「プライバシーマーク制度の枠組み」[注5]という図があり、プライバシーマークの付与認定を受けた企業が、マーク付与機関又はマーク付与指定機関に対して、監査報告を提出する事になっています。付与認定後の実態調査として、「必要に応じて個人情報の取り扱いに関する監査の報告を求めることがあります。」と、説明書には記載されている。

私見：通常、システム監査報告には、その企業の機密に関すること、被監査部門にとって都合の悪いこと等が、指摘・記述されている。システム監査人は、その企業の責任者たる社長宛には提出しても、外部に対して提出する事を想定していないし、外部への提出は、通常、憚れるかと思われる。したがって、今後、

① 本制度でいう監査報告の内容はどの程度の内容、レベルが要求されるのかが不明なので、監査項目、監査報告項目等のガイドラインが必要となろう。

② 当然の事ではあるが、プライバシーマーク付与機関、又は、指定機関では、各企業の秘密が守られる必要がある。

恐らく、監査報告の提出が求められるのは、それなりの理由があっての事と思われるので、余り、神経質になる必要はないかもしれぬが、ちょっと気に掛かる点である。

注5：JIPDECのご好意により、「プラバシーマーク制度の枠組み」掲載の許可を得ている。

VI. 終わりに

「I. はじめに」で記した「天気予報ではゴールデンウィーク中の1日は雨が降る筈だとの事で、その日にちょこちょこPCにむかえば出来るだろうと考えた訳です。」は、正直に白状すると見事に外れました。しかし、頭の中で適当に考えていたことの整理になり、それなりの収穫はありました。本稿が皆様のお手元に届く頃には、サッカーW杯の話題でもちきりでしょう。最後に、余談2つで締めくくる事をお許し頂きたい。

1. EUに関する余談

EU指令(Directive)は、EU構成国を拘束するものであるから、EU加盟国でない日本にとっては無関係だろうと侮っていると、思わぬ情報経済活動への支障が生ずるかもしれないし、グローバル化した日本の経済活動を考えるとEU指令も無視し得ない。個人情報保護では、既述したように「第三国への個人データの移転」で、ECの要求する十分なレベルの保護を図っていないと、EU加盟国の利益を害するとして、是正のための交渉が起こり得る。

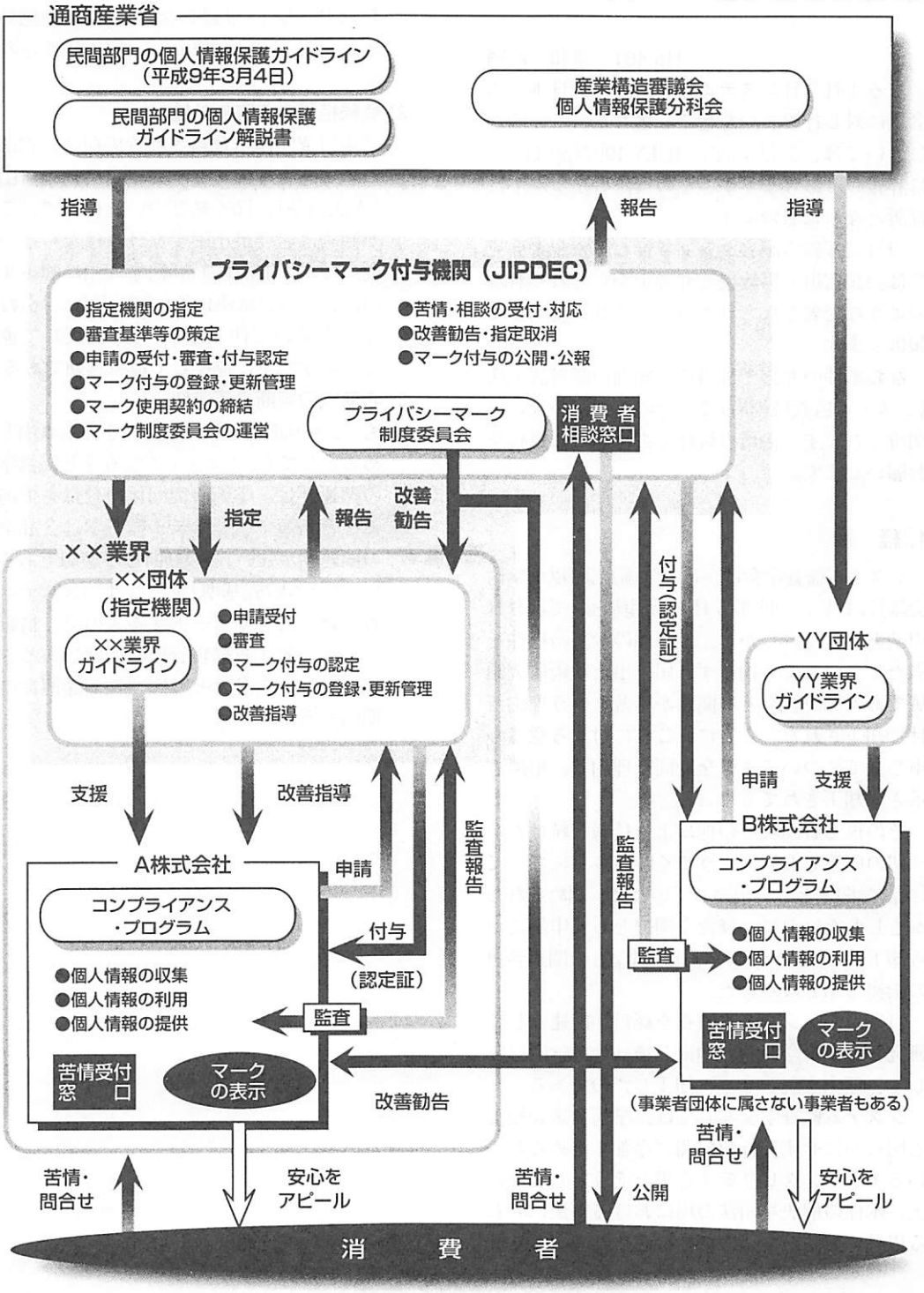
「ひとつの欧州」を目指して通貨統合に取り組むEUは、金融・経済面でも力を増し、従来の米ドル・独マルク・日本円から、今後は米ドル・EUユーロ・日本円となり、日本円の比重はぐーんと下がるのである。余談の余談になるが、通貨だけでなく、EUの力が強い影響力を発揮した例として、4月中旬の新聞で『サッカーW杯入場券「EU共通市場原則で」最後の11万枚売出し』なる記事をご覧になった方もおられると思います。

サッカーのワールドカップ(W杯)フランス大会へ向け、「最後のチャンス」となる入場券11万枚が4月22日に売り出された。昨年中に売り出された入場券の6割は地元フランス向けで、熱狂的なサポーターの多い英国やオランダなどから「われわれ出場国への配分が少なすぎる」と不満が噴き出していた。他の欧州勢からも、入場券の配分につき、「地元フランスを優遇しすぎている」と激しい批判を招き、これにEUが介入しました。EUは欧州での共通市場原則をたてに「地元有利のチケット販売を改めなければ、課徴金をとる」とフランスに厳重警告し、その結果、仏政府と組織委員会は英独仏などEU加盟15ケ国に、ノルウェー、アイスランド、リヒテンシュタインを加えた計18ケ国の居住者である市民にも門戸を開きました。この11万枚に対しては、日本からの申し込みは受け付けられなかった。これと、個人情報保護とは関係ありません。EUの影響力の例を言いたかっただけです。要するに、余談。

2. 真面目な余談

今度は、個人情報保護に関する真面目な余談。プライバシーの侵害、個人情報データの流出の事例は、日本でも多くあり、ここで挙げるのは控えますが、EUにも加盟しているスペインで問題になった事例を述べたい。この事例も4月中旬のニュースで報道されたので、ご存じの方も居られるかと思います。見出しは『軍の勧誘 DMに待った　若者200万人の「名簿」が民間へ スペイン』である。この問題は職業軍人の確保が難しくなっているため、国防省が広告代理店に依頼して「潜在的志願者」の若者をダイレクトメールで勧誘しようと考えたのが始まりだ。スペインでは2002年に徴兵制を廃止し、軍を職業軍人だけの編成に切り替える。ビデオ、ポスター、ちらし、ステッカーをつくるほか、広告代理店に委託して適齢期の男子に手紙で勧誘することにした。スペインには1993年に制定された個人情報処理規制法があり、個人情報の目的外使用や譲渡を禁じ、使った後は完全な管理態勢で保存する場合を除き、破棄を義務づけている。もともと国防省の名簿は、徴兵用に各自治体が義務として提出したもので、法律の専門家は名簿を勧誘目的で使うことにまず問題があるとし、「外部に漏れる心配はない」と国防省が保証するだけでは不十分だと指摘している。国防相は、「法的に問題があると分かれば省内で作業をするか、最悪の場合は断念する」と文書で見解を述べた。

プライバシーマーク制度の枠組み



システム監査学会 日本学術会議を提訴!

No.461 橘和 尚通

去る4月2日システム監査学会は、日本学術会議に対し行政訴訟を起こしました。この問題については、会報No.43、JULY 1997(pp.14-15)に詳報してありますが、その後決着がつかずに提訴となったものです。

当日文部省の記者クラブで行われた記者会見では会長宮川公男教授と弁護士からそれぞれ次のような発表がなされたので、それを要約して報告します。

なお本件の弁護士は当協会顧問の藤谷護人氏(システム監査技術者)で、そのご活躍が大いに期待されます。会員の皆様のご理解とご声援をお願いします。

1. 経 緯

システム監査学会は、日本学術会議(以下学術会議)に対し、一昨年5月学術団体としての登録申請を行った。しかし、その他の全ての用件を満たしていたにも拘らず、届け出た学術研究領域である「経営学」との関連が希薄という理由だけで却下された。さらに、これに対する意義の申し立てについても、全く同じ理由で、根拠も示さず却下されてしまった。

その後も質問状その他による抗議を続けたが一切の応答もなく、ようやく昨年3月になって「会計学関連として申請していれば、認められたかもしれないのに、経営学関連とした申請だから却下した」というのみで、経営学との関連希薄の根拠は示さなかった。

当事者が、システム監査を経営学関連として研究している学問を、学術会議は会計学関連として、理由も説明せずに却下したのである。

システム監査学会としては、学術会議が根拠も明らかにせず、行政機関に今強く求められているアカウンタビリティを果たそうとしない以上、本件の解決を司法の場における解決に委ねる以外に方法がないので、提訴に踏み切った。

2. 訴状の概要

(1) 請求の趣旨

登録申請却下(登録しない)の決定の無効の確認と意義申し出却下の決定の無効の確認。

(2) 登録拒否の違憲無効性

学術研究団体へ登録される権利は、憲法上の基本的人権である学問研究活動の自由権(憲法23条)に深く結びついた権利で、これが制約は必要最小限でなければならない。従って、「関連性の希薄」を理由に却下するのは、学術会議法18条(研究領域は「届け出」で、申請の要件ではない)に違反して違法で、憲法23条に違反して違憲無効である。

(3) 希薄性の判断の不適切

もし120歩譲り、この希薄性を却下事由と認めるとしても、「システム監査学と経営学との関連性は、学術研究団体の登録を拒絶するほど希薄で、システム監査学は会計学との関連性が強い」との判断は不適切である。「システム監査基準」をみれば、システム監査が経営者をサポートするもので、情報システムに対する経営管理の問題であることがわかり、会計学との関連性が希薄なのは明白である。

今月号の会報から二つの連載記事を掲載いたします。

ひとつは、「情報システム部長日誌」です。筆者は当協会当協会の会員ですが、本人の御希望で匿名での連載といたします。某企業情報システム部長としての毎日を題材にした肩肘の張らないコラムを目指すとのことです。

もう一つは、「情報セキュリティーポリシーの必要性と策定方法」で、日本ヒューレットパッカード株式会社の佐藤慶浩氏に執筆を担当していただきます。佐藤氏は、当協会第５４回月例会の講師をお願いした方で、この時のテーマとなったセキュリティーポリシーについて、より詳細に解説していただけるとのことです。

皆様、御期待下さい。(会報担当)

情報システム部長日誌 ー連載　第１回ー

No.999　新城　道彦

自動車部品の製造、販売を業とする当社でも、いよいよISO14001(環境管理システム)の認証を取得することとなった。

国内の製造ラインは東北など長男、長女がまだ地元に残っていて人手が集まる所にあり、その他は海外にいっている。ただし、生産部は依然東京近郊に事務所を構えていて、ここから内外の生産拠点を制御しており、この事務所で取ろうというものである。

当情報システム部は、まだ汎用機を抱えていて、電力消費も大きく、節約の仕甲斐もある部署となっている。

先行して内部監査があったが、いよいよ今日は認証機構の主任監査人が登場しての予行審査ということで、そのオープニングセレモニーに出席した。会計監査人とは、いろいろお付き合いさせていただいているが、環境システム監査人とは初めてである。真面目そうで、厳しさと温かさが同居しており、信頼出来る感じが伝わってくる。

ISOは内部監査を重視しており、14000は特にそうだという。確かに環境管理は永久に続くもので、認証機構としても、そうは付き合っていられるわけではないから、受審団体側が自律的に統制していかなければ実効は期待できないであろう。

会計監査でも内部統制の充実度合いのチェックはある。ただし受審側の個人的な受け取りでいえば、何か傍証固めというような位置付けであるが、14000では内部監査体制のあり方そのものが正面から問われているようである。

セレモニーの後、われわれは職場に戻り、監査人は事務所の中を回られた。夕方、また招集がかかり、結果の発表があった。当社事務局の話では、監査人はごみ箱の中までかき回して分別のチェックをされたという。

結果発表で印象に残る部分があった。

いくつかの部署に対し、「必要な文書が備えられていない」という指摘があった。指摘の表現としては、あくまで「備えられていない」というだけである。ところが、他のある部署に対する指摘では「文書はあるが、それを最新に保つべき手続きが不明確である」ということになっている。

先の、必要な文書を備えていない部署で「ない」というなら「あればいいだろう」とばかりに「ある」だけの状態にして、次の監査を受けると、「最新に保つべき手続きなし」との指摘を受けそうである。今までの日本社会での受審人のいい分では、それなら初めから「文書を備え、それを最新の状態に保つようにせよ」といってくれればいいではないかとなりそうである。

これに対し、こちらの監査人のいい分では「文書を備え、それを最新に保つことは当然のあり方である。文書がない時に、ないという指摘に加え、それを最新に保つようにすべしというのは、監査ではなく、コンサルの領域であり、監査人はそこまで踏み込まない」というものらしい。

「監査」だけでは商売にならず、大きく「コンサル」に踏み込まなければなどといっているシステム監査人からすれば、何ともうらやましい割り切りである。

翌日、汎用機の磁気ディスク装置更新の売込みがあった。当部の担当者は費用低減をいい立てるが、部長のチェックポイントとしては電力消費減もある。当然、減であるという。では、その値は当部のエネルギー減目標に、どの程度貢献するのかと聞けば、ちょっと待ってくれであった。

認証機構の監査は、この後、初動審査、本審査と続く。社内、部内のすべての動きがISOの要求するレベルに至るのも、また道は遠そうである。

「情報セキュリティポリシーの必要性と策定方法」

～企業は従業員(人)による情報セキュリティの維持に、どう対処すべきか～

ー連載　第1回(全3回)ー

日本ヒューレット・パッカード株式会社
マネージング・コンサルタント　佐藤　慶浩

はじめに

セキュリティに関する書籍や資料の中で、セキュリティ方針(ポリシー)という言葉を目にすることがあるのではないだろうか。その言葉の意味から、なんとなく重要そうなものであることは想像できると思うが、それが実際にどんなものであるかが説明されることは、意外に少ない。ここでは、弊社が情報セキュリティ方針策定支援のコンサルティングの提供で留意していることを紹介する。セキュリティ方針の策定を日本企業で現実のものにするためには、その必要性を理解し、セキュリティ方針の定義を日本の組織文化に無理のないものにしなければならない。ここでは弊社の考える日本企業におけるセキュリティ方針の策定と運用について解説する。

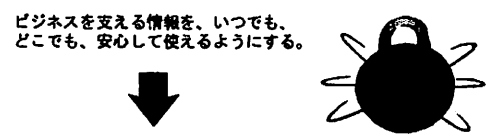
セキュリティ方針のレベル

セキュリティ方針とセキュリティポリシーはまったくの同義である。しかし、セキュリティ方針と言った場合、その定義にはレベルがあって、企業全体のセキュリティ方針、それから部門のセキュリティ方針そしてコンピュータシステム単体のセキュリティ方針というように様々なレベルがある。これらのレベルを正しく理解しておく必要がある。それらのレベルは3段階に大別できる。もっとも下のレベルは、装置やソフトウェアなどの方針に関するもので主として技術的なことだけを言及するものである。これに加えて、運用や管理方法などのプロセスまでを含めた2番目の段階のレベルがある。日本で多く知らているのは、この段階までである。しかし、この段階では人々の行動規範までは言及しないため、それについては通常は非電子的情報を対象とする既存の規定文書などを拡大解釈して済ませることになる。しかし、今日の情報システムはビジネス活動と密接なものとなっており、例外処理の発生するビジネスの現場においては、ビジネス目標の達成と情報セキュリティ維持とのトレードオフを個人が判断することは、技術やプロセスとは異なるセキュリティの問題を生み出している。この問題を人的領域として方針化するのが、3番目のレベルである。技術とプロセスと人を扱う、この最上位に位置するセキュリティ方針を情報セキュリティ方針という。本書では、この企業全体の情報システムに関するものという定義での「情報セキュリティ方針」について説明する。

情報システムの目的

情報システムの目的は、ビジネスを支える情報をいつでも、どこでも、安心して使えるようにすることである。情報システムそのものは情報の隠蔽を目的とするのではなく、積極的な情報開示や共有をするための基盤である。積極的な情報の開示や共有をするための手段として情報を保護する必要があるが、保護することが目的ではない。情報セキュリティは、定められたセキュリティの要件を満たしつつ、積極的な情報の開示、共有をするために、貴重な情報を正しく守るということである。

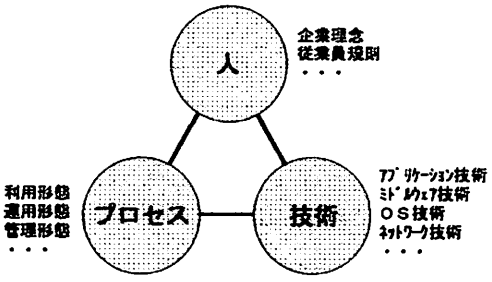
情報システムの目的



情報システムは、情報の隠蔽を目的としない。
積極的な情報の開示／共有をするための基盤です。
情報セキュリティは、積極的情報利用を現実のものとするために、情報を適切に保護します。

従業員のアクセスが制限されるものは社内の全電子情報の10%にも満たないのではないか。当社のなかではもっと低く、全電子情報のうち全従業員が共通に見れないものは5%くらいである。ほとんどの情報は従業員が見れる、そのうちお客様に提供することができる情報が8～9割を占めている。このように、情報の保護ではなく情報の開示／共有を目的として情報システムがあると考えている。

情報システムの構成要素



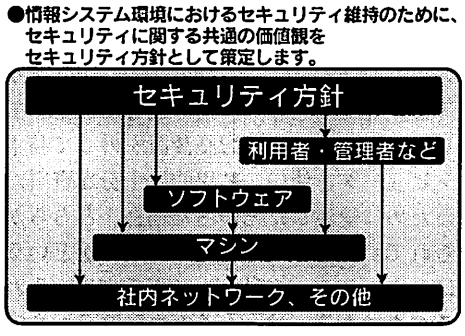
情報システムの構成要素

情報システムの構成要素を考えると、ハードウェア・ソフトウェア、アプリケーションなどの技術があり、これを使うのが人で、人が技術をつかうためにプロセスがある。技術に関しては、アプリケーション技術、ミドルウェア技術、OS技術、ネットワーク技術などがあり、人に関しては、たとえば企業理念とか従業員規則などがつかさどっている。人と技術を結び付けるものとしては、コンピュータの利用形態であり、利用形態から利用手引書があったり、運用手引書、管理手引書があるということになる。情報システムは、技術・人・プロセスから成り、人が絡んでいることを忘れてはいけない。

セキュリティ方針の位置づけ

人が絡むことから、最初に必要となるものがセキュリティを維持するための共通の価値観である。セキュリティとは何なのかという価値観、それを定めるものがセキュリティ方針である。メインフレームのようなホスト型情報システムでは、ユーザのできることは限られていた。システムの開発者が設計した画面の中で、決められた手順で情報を処理していた。このためシステム管理者がセキュリティ上好ましくないと考えることは、その手段を提供せず、また、手順書においての禁止事項として細かく指示することができた。つまり、集中的な制御が可能であった。しかし、近年のオープンシステムを組み合わせたシステムでは、ユーザの自由度は飛躍的に広がっている。例えば、業務連絡や社外の取引先との連絡に電子メールを使うといった場合、機密情報が社外に流出することは、故意にも過失にも容易に起こり得ることである。電子メールを技術として使い、それで業務連絡というプロセスを実現した場合、セキュリティの維持には「人」が重要な要素として関わってくる。情報システムが特化型のものから、より汎用化したものにある傾向は、近年のビジネスの目標達成に必要なことである。汎用化することは、ユーザによるシステム利用の自由度があがったことを意味する。以前のように画面上のエントリ内容を制限することで、集中的に制御することは困難になったのである。このような環境において、セキュリティ維持をするには、技術や手順だけを制限するのではない、もっと人の行動規範に視点を向けた枠組み、すなわち、情報セキュリティ方針が必要である。

セキュリティ方針の位置づけ



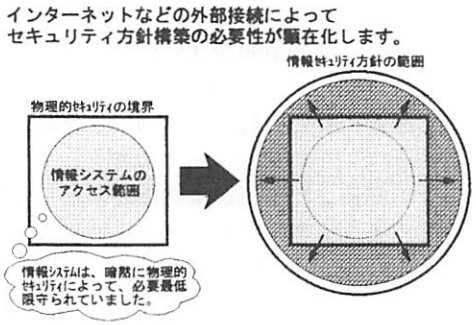
情報セキュリティの背景

情報システムのセキュリティは元来あたりまえのものであり、コンピュータが出てきたときから既に存在していた。1950年代にホストコンピュータが商用で使われ始めたときからシステムのセキュリティは誰かが考えてくれていたわけである。しかし、物理的に外部と遮蔽された環境においては、従業員の個人的なモラルや技術力に依存したセキュリティの維持はある程度機能していても、インターネットなどによって外部と接続されるようになると十分ではなくなる。企業に損害を与える要因が多くなってくるからである。

セキュリティ方針の必要性の顕在化

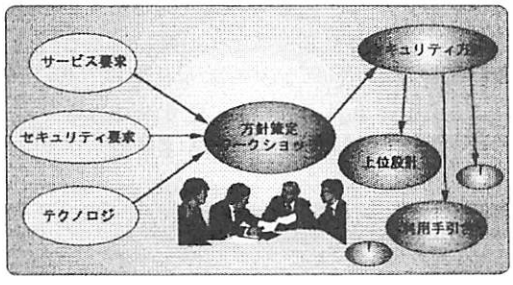
従来のホストコンピュータシステムでは、基本的に情報システムのアクセス範囲は物理的なセキュリティの境界の中に存在していた。物理的なセキュリティの境界とは建物のセキュリティや警備員などである。その中にいる限りは

セキュリティ方針の必要性の顕在化



情報システムは暗黙に必要最低限は守られていた。たとえば社外秘の情報を机の上に置いていても、建物自体は警備会社によって保護されているために、それが社外の人に見られるということはない。電子情報も同じで、物理的なセキュリティの中にある限りはある程度ルーズであってもまず問題にはならなかった。しかし情報システムのアクセス範囲が広がってきて物理的なセキュリティの境界を越えてしまうようになると、情報セキュリティとして守る壁を用意しなければ攻撃の対象になってしまうことが起こってきた。情報セキュリティというものを利用者個人が直接考えなければいけなくなり、セキュリティ方針策定の必要性が顕在化してきたわけである。

セキュリティ方針作成の流れ



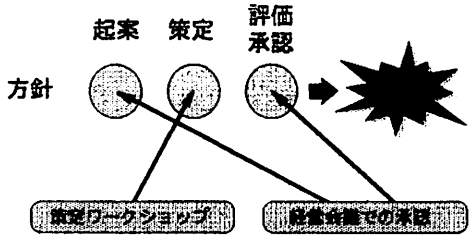
セキュリティ方針作成の流れ

セキュリティ方針を策定するには、サービス要求とセキュリティ要求をバランスさせることが必要である。たとえばインターネット接続をして社外とメールをしたい、あるいはwebから情報を取ってきたいという場合、インターネットに接続して社外から全く攻撃を受けなくするという解はない。そのためにはインターネットに接続しないということだが、そうするとサービスが成り立たなくなる。このバランスを取るためにテクノロジーが介在する。すなわちファイアウォールというテクノロジーができたからインターネットに接続してもセュリティがある程度守られて、社外と電子メールのやり取りができるわけである。セキュリティ、サービス、テクノロジーの3つのバランスを考えながら検討を進め、出来上がったものがセキュリティ方針となる。このセキュリティ方針がユーザ向けの利用手引きやアプリケーションの開発指針(ガイドライン)に展開される。

重要なことは、サービス要求が本当に満たされるのかについての同意を十分に取っておくことである。たとえば、一番厳しい認証の仕組みとして全ユーザが個人認証を受けるとする。いったん認証されればその人は権限を与えられた情報にいくらでもアクセスできサービス要求は満たされるが、認証を行っているセキュリティサーバーがダウンしたときに何が起きるかを想定しなければならない。全ての情報にアクセスできなくなり、手元のPCすら使えなくなった場合にどう対応するかは、非常に難しい問題である。明日までに営業活動用の資料を作らなければいけないのに認証システムが壊れた時、一人は、会社のセキュリティ方針として認証ができない限りはコンピュータリソースを使ってはいけないということなので、それを守り、知っている範囲内でワープロ書きだけをして失注した。別の一人は、認証装置を外して勝手にコンピュータを使い、結果的に十分な資料が作れたために受注したといった場合、どちらが責められて、どちらが誉められるべきかということはセキュリティ方針として事前に規定されているべきである。せっかくセキュリティを守っ

ても営業成績が悪いとういことで査定が悪くなったとしたら、セキュリティ方針を守ることがばからしいことになってしまう。この部分のバランスも考えておく必要がある。

セキュリティ方針決定までの流れ



セキュリティ方針の決定までの流れとしては、方針を起案、策定して、評価、承認の手順となる。経営会議レベルで評価、承認されないと企業全体のセキュリティ方針にはならない。経営会議レベルの承認が必要なものであれば、とにかく全部作って、後で経営会議に付議しようということは通常の企業のプロセスとしてはありえない。まずは起案の時点で経営会議で承認をもらっておかないと、作業が無駄になってしまうことがある。

明日の営業利益とセキュリティのどちらを取るかといった場合、それが現場任せになってはいけない。これを解決するためには経営会議レベルでの承認が必要である。

セキュリティ方針は、企業におけるセキュリティ目標についての経営陣からの意思表明である。

セキュリティ方針と規則集との違いは、規則が単に従業員に対して行動を強いるのに対して、方針は従業員に対する支援体制が示される点である。

近畿会だより

No.299 安本 哲之助

セキュリティ問題の徹底討論を合宿でやろうとのことで第56回の近畿会システム監査定例研究会は3月6日から敦賀地区での1泊研究会となった。

テーマは「原子力発電所の見学と情報システムの脆弱性を考える」と銘打ち、第1日目は関西電力美浜発電所見学会、第2日目は討論会「情報システムの脆弱性について」とし、コーディネータは川端純一氏(敦賀市役所)、問題提起者は神尾博氏((株)クボタシステム開発)と松田貴典氏((株)日本ユニシス)の両氏にお願いした。

はじめに

今回の研究会はまず最高レベルのセキュリティ諸対策が具現されている原子力発電所を見学し、情報システムの脆弱性の見直しを行おうとの構想であり、今までの公開シンポジューム等で会員同志交流のあったシステム監査学会関西地区研究会との共同開催の研究会とした。

この計画はかねてから準備をすすめていたが、昨年の福井県の原油漂着事故などでやむなくくりのべとなっていたのもであり、今回会員である敦賀市の川端純一氏のご尽力でようやく実現した。

年度末の業務多忙期であったがセキュリティに関心の深い20名の会員の参加を得て、有意義な研究会となった。なお、中部支部からも斎藤礼三郎氏の参加があり、にぎやかな研究会となった。

第一部 関西電力美浜発電所見学記

福井県敦賀地区には原子力発電所が数箇所あるが、この発電所は3基の原子炉で現在フル操業されており、発電した電力は京阪神地区へ送電されている。

ここは先年、原子炉の中枢部である蒸気発生機の細管破断事故をおこし、新聞紙上をにぎわした2号機を有する発電所で、すでに修復工事も終わり正常に再稼働されている。

今後の事故の再発防止に役立てる意味で当時の事故関係の資料を蒸気発生機の現物ともども特別施設を設けて常時展示公開し、事故情報の

開示に懸命に取組まれている。

企業にとって不都合な情報であっても開示し、安全運転へ真剣に取組んでいる様子を拝見し、敬服に値するものとの感を深くした。

直接の事故原因は発電機の心臓部である蒸気発生機の検査不良にあったと考えられ、通例では考えにくいミスであるが、複合要因がかさなった場合や検査技術が未熟であれば起こりえたのかも知れないとの見方もあった。さすがセキュリティに関しては入退出管理は完璧に実施されており、監査人からの質問の余地はなかった。

この施設は地域との調和を最重点に運営されており、住民への広報対策に配慮し、一般見学者にも丁寧に説明がなされていた。また、この施設の原子力運転員は多額の研修経費をかけ10年間の訓練をへてようやく一人前になるとの厳しい訓練コースをへているので安全な運転が行われている点を強調されていた。

この研修費用の主要なものはコンピュータシュミレーション経費が大きな部分を占めているとのことで、ここでも制御系コンピュータが大きな役割をはたしていることが理解された。しかし、これほど訓練をかけないと一人前にならないいわば人に依存した部分が存在することは、逆に難しい課題をはらんでいるとも考えられその運営のご苦労がうかがわれた。

この施設の設備関係の整備は見事なまでされており、今この職場の悩みは設備の複雑さや経年劣化よりも「人」にかかわる課題が永遠の課題であり、現場では「なくそうヒューマンエラー」のキャッチフレーズがかかげられており、懸命な取組みがうかがわれた。

セキュリティの究極の課題は「人が持つ弱さ」。人の勘違いや疲労による見落とし、この程度はいいだろうとの判断ミス等「ヒューマンファクター」が課題であり、情報システム環境においても同様であることが再認識できた。関西電力さまには別途質疑応答の機会を設けていただき私どものぶしつけな質問にも誠意をもってお答えいただき、一同深く感謝している。

翌日の第2部では情報システムの脆弱性について徹底討論を行い、議論百出で司会者もとまどう活発な意見交換がなされた。なお、研究会終了後もなお、引き続き脆弱性問題では電子メールによる継続討論もなされ大変有意義な研究会であった。

第2部の経緯はまた紙面をあらためて報告する。

近畿会　第57回定例研究会報告

No.780　蘆田　好実

今回の発表は汎用機から分散機システムにかわりつつある情報システムの潮流の中で、システム監査人一同が分散システム環境をどのように監査するか腐心・注目しているテーマであったため、会場あふれるばかりの多くの参加者があり、後半の質疑応答も活発な研究会となった。

1. はじめに

4月17日の近畿会第57回定例研究会において、IBMのユーザー団体である日本ガイドシェアの97年度研究成果である「分散システム監査実施のガイドライン」について報告させて頂きました。当該活動は1年間のプロジェクトチームを編成し、多方面にわたる情報システムの効率的利用方法の研究を目的とするメンバーの自主的共同研究活動です。今回のテーマは96年度の活動成果を踏まえてシステム監査人が「システム監査基準」に準拠して分散システム環境を監査する際のガイドラインとして整理したものです。

以下は発表要旨です。

2. 課題検討の流れ

分散システム環境のガイドラインを整理するにあたり以下の4つの領域について検討を進めた。

・通産省〔システム監査基準〕に対する評価と提言
・分散システムにおけるリスク分析
・分散システム監査のために必要なコントロール
・現状の監査基準への適用評価

3. 通産省〔システム監査基準〕に対する評価と提言

システム監査基準に対して『具体性の欠如；基準項目の不足；基準項目の重要度が不明確；狭い対象範囲』といった問題点を指摘し、この問題点に対し『システム監査基準の具体化と実践性の確保；実施基準項目の充実；実施基準の重要度の設定；システム監査基準適用範囲の見直し』を96年度に研究グループとして提言した。97年度はこの提言の具体化のため分散システム環境の監査ガイドラインを実務に適用できるものとして新たに作成した。

4. 分散システムにおけるリスク分析

まず、分散システムにおける『企業に損失をもたらす脅威(6グループ)』と『企業が守るべき保護対象(8グループ)』を整理し、これらの組合せから分散システム特有のリスク傾向(10パターン)を導き出し、必要な監査ポイントを明確にした。

5. 分散システム環境監査のために必要なコントロール

分散システムにおける監査ポイントを分散システムに必要なコントロールとして以下の27項目に整理した。『ライブラリコントロール；フィジカルアクセスコントロール；変更管理；ウイルス対策；IT資産管理; ライセンス管理；外部接続管理；ロジカルアクセスコントロール；ネットワーク設計基準；導入・運用手順；ソフトウェアバージョン管理；障害回復手順；障害回復体制；全社的情報化投資計画；開発手法とプロジェクト管理の標準化；用語の標準化；ベンダーマネジメント；ビジネスコンティニュイティプランニング(災害対策)；アプリケーションインベントリー管理；アプリケーションシステムの有効性検証メカニズム；IT投資／購買の要求承認基準と手続き；役割分担と責任の明確化とSOD；社外情報機密区分とその取り扱い規定；不正アクセスエラーの検出；データインテグリティの確保；エンドユーザーデータの取り扱いルール；プライバシー保護』

これらのコントロール(監査ポイント)はシステム監査基準から導き出したものでなく分散システムで起こりうるリスクを回避するために必要なコントロールとして考えた。そして、情報システムの健全性を確保するためにはそのコントロールの有効性を保証する(確認する)必要がある。

6. 現状の監査基準への適用評価

次に、システム監査基準をベースにして、これらのコントロールが監査項目として導き出せるかを検証した。結果としてシステム監査基準からこれらの27項目全てを具体的に導く事は困難であり、96年度の指摘通りシステム監査基準の本基準だけでは実際の監査項目を設定するのは無理があり、細分化が必要であると判断された。これはシステム監査基準を否定するものでは無く、システム監査基準が全ての情報システムを対象に整理されているため一般性が求められているためと理解される。そのため、今回の検討結果の様に監査対象の目的にあったシステム監査基準の下位基準(具体的詳細基準)が実務上必要であると考えている。また、「システム開発取引の共通フレーム」のライフサイクルに準拠した構成では、開発プロセスに沿った監査では有効であるが情報システム全般のコントロールを監査するケースへの適応は困難であると評価される。情報システム全般のコントロールを監査する項目の更なる充実が必要と思われる。

7. 分散システム監査基準(監査チェックシート)の作成

これらの結果をもとに27項目のコントロール単位に監査チェックシートを作成した。これらのチェックシートは監査目的にあわせて監査ポイントの設定(脅威と対象の組合せ)をおこなうことにより有効に活用できるよう構成されている。

8. おわりに

今回の研究活動を通じてシステム監査人の視点では無く、現場サイドに立った監査ポイントからの整理を行うことができた。実際監査をおこなう場合、システム監査基準だけでは監査を組み立てる事も困難であり、今後今回のような下位基準を充実させていく事がシステム監査の実施の価値を高め、これが普及に貢献することになるとのプロジェクトメンバーの統一した意見であった。

今回の研究会には約30名もの会員が参加し、色々な視点で討議や意見交換が活発におこなわれ大変有意義な時間を過ごす事ができました。この場を借りて御礼申し上げます。

中国支部だより

No.387 安原 節男

新しく四国の会員の方も支部構成員になられ、さらに新会員として"後藤知久"さん(株)セシール=788=、"西村隆"さん(株)中国日本電気ソフトウエア=802=の、お二人をお迎えし、計22名と賑やかになりました。

しかし、会員の分布状態をみると、島根・広島・岡山・香川・高知と極めて広域となり、なかなか、お顔を会わせる機会をつくることも大変です。

そんななかで、5月上旬に、支部のE-Mailの「メーリング・リスト」を開設しました。アドレスは<saajc@hiroken.ne.jp>です。リストには、私が把握できた範囲は登録していますが、未登録の方は<off an@hiroken.ne.jp >あてに、アドレスをお知らせください。

話題は変わりますが、今年も、「システム監査企業台帳」への登録申請の時期となりました。恥かしながら、今年も、当社〔(有)オフィス・あん〕は昨年に続き登録申請します。昨年来、ことに監査費用は見積らず、期間的な制約も明確にしない監査を続行しており、その継続実績を申請します。

どなたか、無報酬ですが、監査のお手伝いいただける方がいらっしゃれば、ありがたいのですが。(すこしムシのいい話ですが……)

九州支部だより

No.307 行武 郁博

九州支部の活動は毎月の例会のみですが、会員の皆様の協力により現在のところ毎月開催しています。

4月の例会では「PLと改正民事訴訟法」大羽宏一・林田学著(日本経済新聞社1997.10月刊行)を紹介いたしましたのでご参考までにその概要を報告致します。

平成10年1月より改正民事訴訟法が施行された。改正の主眼は訴訟の容易化、迅速化であり、訴訟王国であるアメリカの法律が多く取り入れられた。今後は改正民事訴訟法の下でのPL訴訟の増加が2、3倍になることが予想される。このような前提で、本書はPL訴訟の諸外国や我が国の状況、改正民事訴訟法がもたらすPL訴訟への影響、また企業のPL訴訟への対応等を論じたものである。日頃、馴染みのない訴訟法の分野であるが改正民事訴訟法の改正の要点が判りやすく書かれている。また、民事訴訟法とシステム監査は直接結びつくものではないが、システム監査人に対してシステム監査の新たな視点を示唆しているように思われる。

改正の要点は次の5点である。

1. ディスカバリーへの接近

アメリカの訴訟は証拠を集める段階と陪審員の前で証拠を調べる段階に分かれており前者がディスカバリーといわれている。ディスカバリーではインタロガトリーという質問書を発し、回答を得ることで訴訟の照準を定める。改正民事訴訟法はこのインタロガトリーに似た制度として当事者照会を導入し、文書提出命令の範囲を広げた。

2. クラスアクションへの接近

一人または複数の原告が、損害賠償訴訟において共通点を持つ一定範囲の被害者(クラス)全員を代表することが許される訴訟手続制度である。改正民事訴訟法では選定当事者の追加といういわば、擬似クラスアクションであるが、PL訴訟のように同じ被害者が多く発生しているケースで多用される可能性がある。

3. 損害額立証の軽減

原告側が、損害賠償を請求するのであれば、その損害額は原告が立証しなければならないが、それが困難な場合に、裁判所が口頭弁論の全主旨及び証拠調べに基づいて相当な損害額を算定することができる。つまり、性質上、立証困難な損害額については厳密な立証を求めないということであり訴訟の提起がやりやすくなると思われる。

4. 小額訴訟制度の新設

請求額が50万円以下の事件については、一回の審理で判決を下すものである。訴訟の迅速化が期待されるものであり、アメリカの訴訟制度に倣って導入されたものであるが、被告には通常の訴訟を選択できる点が問題とされる。

5. 最高裁への上告制限

最高裁へ上告できる場合は、憲法違反と重大な手続法違反に限られ、それ以外のケースは判

例違反等重要な問題を含むと最高裁が認めた場合のみ上告が許される。実質二審制となり訴訟の迅速化が期待される。

以上の改正で、特に注目すべきは1.ディスカバリーへの接近の文書提出命令である。文書提出命令とは、相手方や第三者が所持する文書を証拠として使いたいときは裁判所が文書の所持人に文書を出すように命じるものである。この対応如何によって訴訟の勝敗が大きく左右される。旧民事訴訟法でもこの命令はあったが極めて間口の狭いものであった。改正民事訴訟法ではこの間口を大きく広げ、企業が所有する文書は原則としてすべて提出しなければならないとした。提出を免れる文書は単なるメモ等の自己使用文書、秘密文書とされる。

ここでは、企業はいかなる文書を所有しているかという情報が重要なファクターとなる。それは文書管理規定、監査役監査文書、行政提出文書や法定保存文書またISO9000シリーズ等の登録企業ではISO対応作成文書により推定されるということとなる。本書では文書提出命令への対応として次の3点を挙げている。日頃の文書管理が極めて重要ということである。

1. ワードマネージメントの励行

企業内で作成する文書は常にディスカバリにより公になる可能性があるという意識で作成することである。アメリカでは、保存する予定の文書については技術者が作成した文書は社内弁護士がチェックしているとのことである。ISO9000シリーズ等の登録企業の場合は作成保存文書が公になっているので留意すべきである。

2. 文書廃棄ルールを明確にする

文書廃棄ルールを定める。そして保存期限が到来した文書は確実に廃棄処分を励行する。

3. 職業秘密文書の作成・管理

職業秘密文書を作成し、管理する。何が職業秘密に当たるかは不正競争防止法の営業秘密が参考になるとされる。秘密管理性、有用性、非公知性が必要とされるが本書ではさらに第三者に開示する際の秘密保持契約を結んでおくことが必要であるとされている。

「所感」ーシステム監査の対応についてー

システム監査は企業等の情報システム全般を監査の対象としている。当然情報システムの企画、開発から運用保守にいたるまでの数多くの文書が存在する。その殆どは自己使用文書とも職業秘密文書ともいえない文書であろう。そうであれば不幸にして訴訟という事態が発生した場合は文書提出命令をうけて公になる文書である。このような事態を予想した記載内容や表現等についての事前チェックが必要であろう。また、最近では、ISO9000シリーズ等の登録企業が増加しているが、当該企業が作成・保存文書の情報は詳細に亘って対外的に公知されているものである。ISO9000シリーズでの認証では、文書の内容まではチェックされないということでありそうであればなおさら内容のチェックが必要となろう。ISO9000シリーズ等の登録はある意味では、両刃の剣であることを弁えておくべきであろう。

改正民事訴訟法は、これからのシステム監査に新たな視点からの監査の必要性を示唆しているように思われる。

以上は本書の一部の概要照会に過ぎません。興味のある方には本書の一読をお薦めします。

第55回月例研究会聴講報告

開　催：平成10年1月23日
テーマ：「電子認証サービスの現状と将来」
講　師：日本ベリサイン株式会社
取締役営業本部長
外川　政夫氏

No.608　三谷　慶一郎

第55回月例研究会では、エレクトロニックコマース(EC)普及のために、極めて重要であるといわれている「電子認証」をテーマに取り上げ、国内における代表的な電子認証サービス企業である日本ベリサインの外川氏にお話を承った。

以下、講演の概略を報告する。

1. インターネットにおけるセキュリティ

- インターネットユーザの急激な増加と共に、インターネット上でのビジネスの市場規模は大きくなりつつある。
- 一方で、ネットワーク犯罪やセキュリティ問題も激増しつつある。
- 「ネットワーク上での情報の盗聴・改竄」「本

人のなりすまし・否認」といった脅威への対策として電子認証が注目されている。

2. 電子認証に使われる暗号方式

・暗号化技術には「共通鍵暗号」「公開鍵暗号」があり、前者には鍵配送時のリスクが、後者には暗号化処理速度が遅いという欠点が存在する。
・電子認証は「公開鍵の持ち主」が誰かを証明してあげることをいい、客観性を持たせるために、第三者機関がこれを行う方が望ましい。

3. 認証機関の役割・機能

・認証機関は「認証証明書発行時の本人確認」「証明書の発行管理」「証明書のディレクトリサービス」といった役割を担う。
・ベリサインの認証証明書には保証のレベルに応じてクラス1からクラス3までの3種類がある(法人認証はクラス3のみ)。

4. ベリサイン認証センターの運営

・システムを取り巻く脅威から認証局の安全性を保証するために、災害・故障・過失・故意に対して、各々強力な対策をベリサインでは実施している。
・また、認証局運営に関して、外部の監査機関から定期的な監査を受けている。
・認証局を運営するための「憲法」としてCPS(認証局運用規定)を設定している。
・消費者保護のために、NetSureという認証保険にも加入している。

5. 米国での認証サービスの現況

・Business to Business、Business to Consumer、Government to Citizen、Enduser to Enduser、といった多くの場面で電子認証サービスは適用されると考えられる。
・証明書発行サービスには、パブリック型認証サービス(独自ブランドでの証明書発行)と、プライベート型認証サービス(顧客仕様に応じてカスタマイズした証明書の発行)の二つの形態がある。
・米国ベリサインでは、Netscape, Microsoft, VISAinternational 等の法人顧客に対してサービスを行っている。

6. ベリサイン社の今後の取組み

・米国ベリサインでは、「グローバルビジネスの展開」「ECマーケットの新規開拓」「業界標準の確立」「消費者にやさしいサービスの実現」を目指して今後も取り組んでいく。

7. 電子認証サービスの展望と課題

・セキュリティの面から見たICカードの有用性は極めて高い。
・パソコンのスマートカードに認証証明書を入れておくようになるだろう。
・暗号輸出規制やキーリカバリー構想、あるいは電子認証におけるその他の法律面の整備(電子保存体の証拠能力、電子署名契約の法的効果)といった行政の動きについては今後注目していきたい。

第56回月例研究会聴講報告

開　催　平成10年3月20日
場　所　労働スクエア東京
テーマ　「大蔵省・通産省におけるシステム監査の取り込み動向」
講　師　日本ユニシス(株)ITコンサルティング室
当協会副会長　荒川　幸式氏

No.526　富山　伸夫

はじめに

今回より、研究会の会場を日比谷線八丁堀そばの労働スクエアに移した。交通の便がよいこととテーマ・講師に期待感が高かったことにより、大勢の参加者があって熱心な討議が行われました。会場はゆとりがあって、照明やOHPの便も良く、なによりも会場費が非常に安いので、今後はここを中心に研究会等が行われることになるそうです。

講演要旨

1. 金融検査庁の発足

大蔵日銀等の金融中枢部門の不祥事がにぎやかに紙面を汚していますが、金融監督の正常化はきちんとやっていただかなくてはなりません。平成9年6月20日の官報でそのための金融監督庁の設置が公布されています。検査部門の分離独立ということですが、従来より非常に幅広い範囲の金融機関を検査監督することになります。このために、職員は現在業務を含め100人

のところが400人体制となります。

2. 金融検査チェックリストの公表

平成9年1月末に、大蔵省から「コンピュータシステム及びコンテンジェンシープランのチェックリスト」を公表するという新聞発表がありました。この趣旨説明によると、従来部内で行ってきた金融検査のチェックリストを公表することによって、各金融機関が自己責任の原則のもとで、個々の実情に応じて自らの体制整備をして、システム監査をも行うものとされています。

このチェックリストは、本部・コンピュータセンターでの通常時チェック項目と非常時のチェック項目、コンテンジェンシープランチェック項目、営業店での通常時チェック項目と非常時のチェック項目としてまとめられています。しかしこの中身は項目が大括りであるうえ、センターと本部各部門を一緒にしているところがあり、実際に使うとなると、少し手を入れないとチェックリストとして使いづらいものとなっています。

また、大手都市銀行や地銀上位行は、FISCの基準で内部検査としてシステム監査を前からやっていますが、下位行や第二地銀では、十分とはいいがたい状況にあります。

チェックリストの中のシステム監査・内部検査体制の項に「システム部門から独立した部門あるいは外部のシステム監査人への依頼によるシステム監査を行っているか」という項目があります。そこで、大蔵省に「外部のシステム監査人の要件は」と尋ねてみたところ、システム監査技術者とは言ってくれませんで、「しかるべき有資格者」とのことでした。通産省の担当課にこのことをお話しすると、「既成事実となるよう頑張って下さい」と言っておられました。

このチェックリストを使えるようにブレークダウンすると、200頁近くのものになります。日本ユニシス社でこれを作成し(出席者に回覧あり)、各金融機関に対しDMを出して監査の提案をしています。はじめは検査部長さんにあてて出しましたが、ほとんど反響がなく、それがシステム部長さんに回って、そちらから問い合わせがくるようになりました。

3. 2000年問題など

また大蔵省では、平成9年12月24日に「コンピュータ2000年問題に関する金融検査におけるチェックリスト」も公表しています。2000年問題は、マイクロプロセッサを積んでいる全ての機器とシステムに関係しますから、チェックしきれずに相当な影響が出るだろうと言われています。国際的にも各国政府機関が取り組んでいます。

大蔵省の他に日本銀行ではもっと詳しいチェックリストを出しています。日銀は実際に大型コンピュータを運営している関係もあり、コンピュータに強い。日銀考査は、以前は契約に基づき拘束力がやや弱かったのですが、今後は改正日銀法で強制考査ができることになるので、このほうからの監査圧力が効いてくるかもしれません。

そうはいっても大蔵省のチェックリストは、最初は経営レベルのコントロールを監査することとなっていまして、内部監査人や外部監査法人では突っ込みにくい項目を挙げているあたり、なかなかのものといえます。米国では、経営コントロールのレベルが格付け機関の指標となるようですから、日本も近いうちにあたりまえのことになるでしょう。

ところで、大蔵省検査の実態ですが、いろいろと面白おかしく情報がでておりますけれども、原則は抜き打ち検査です。トップヒアリングから始まり、業務検査、コンピュータ検査、営業支店検査などがあります。コンピュータ検査は、担当官によりばらつきが大きいのが実情です。しかし、これからは検査専門機関の中での人事異動しかないわけですから、システム監査の事例を積むことによって、レベルが上がってくると思われます。

4. システム監査人の職域拡大

一方通産省の動きとしては、平成9年7月8日付け官報で「情報処理サービス業電子計算機システム安全対策実施事業所認定規程」の改訂を出しています。これは規程の中に「電子計算機システム」とあるのを「情報システム」と用語を変更したことのほかに、認定用申請用紙にシステム監査人の保有資格名称記入欄を新設しています。ここでの資格については、聞かれたらシステム監査技術者が望ましいと指導しようということになったようです。なお、この規程は平成10年4月1日より適用となっています。

また、3月12日の朝日朝刊によれば、あいつぐ金融不祥事に危機感をもった自民党から金融検査士の導入構想が出てきました。これは金融検査庁だけでは数多い金融機関の検査を賄いきれないから、民間に公認会計士のような金融検

査をゆだねることが出来るようにしようというものです。そうすると金融検査の一部としてシステム監査が必要になりますから、金融システム監査士といった職域が出てきて、今のシステム監査技術者から進める道ができるかもしれないわけです。

こうした事情から、日本システム監査人協会としては、自民党の金融不正防止特別調査部会の会長である野呂田代議士に対し、「金融システム監査士＝システム監査技術者」であることを認識してきただくために訪問する予定です。

質疑応答

Q：監査料金の相場としてはどれくらいのものでしょうか

A：企業規模によってもちがいますが、当社がDMで金融機関に提示している金額は、コンピュータシステム監査300万、コンテンジェンシープラン監査200万、2000年問題監査100万としています。

Q：チェックリストを使う時期として、例えば2000年問題などどうゆう時期が適切か

A：運用の監査は定期的に行うが、2000年問題は今が問題で、様子を見ていて遅れてしまいましたでは意味がありませんから、早めに実施することが望ましいです。

Q：チェックリストによる監査の責任範囲

A：監査責任は原則として無限責任ですから、監査ミスにより損害が出たとなるとおおごとです。通常の注意事項を守って監査がおこなわれたと言えるのであれば免責されると考えられますから、あとでそう言えるだけの証拠となるものを収集しておかねばなりません。さらに当社は「監査フィーの範囲で損害を弁償します。」という条項を入れて契約しています。

Q：2000年問題で「社外ベンダー会社から安全確認を文書でとれ」と言われていて、なかなか難しいのでどうしたものか

A：文書で貰う努力をしていたという記録を残しておくといいと思います。

受講後の感想

非常に分かりやすくためになる話でした。システム監査人の職域拡大のチャンスにつながるから協会としても頑張らなくては、という感じがしました。

(追記)お話の中でこんな情報がありました。

1. 大蔵省の外部公表用のホームページアドレスは、次で今日の話も出ています。
   http://www.mof.go.jp
2. 2000年は閏年、2100年は平年
   閏年は4で割り切れる年が全てかと思っていましたが、100で割れる年は平年で、さらに400で割りきれるとまた閏年になるそうです。

事例研究会活動報告
ーY社システム監査の感想ー

事例研究会

No.562 森本 哲也

ふと睡魔に襲われた午後のひととき、クライアントからお預かりした資料を処分した。シュレッダーで書類を裁断していると、これで終わったのだなと、達成感が満ちてきた。いつもながら終了後の不要文書処分は、大好きな仕事である。

まずは、切磋琢磨し合ったトレーに仲間、リーダー及び先輩のチームメートに感謝いたします。

92年度の試験でシステム監査技術者試験に合格したものの、実際に監査を行う機会がなく、少々焦りを感じていた。たまたま昨年度の協会年次総会の折り、事例研の幹部の方と話す機会があり、早速仲間に入れていただいた。昨年の秋に模擬監査を体験するセミナーで基礎を学び、今回の臨床講座に参画した次第である。順調な学習課程でわだかまりもとれ、会社の業務で監査をアサインされても何とか対処できると感じられるまでにスキルアップした、と自己評価している。身に付きだしたスキルを固定させるため、次の監査にも是非加わりたいと願っております。

以下に初体験として参画したY社システム監査の経験を拙文にまとめました。協会の方々の参考になれば幸いです。

1. 報告の骨子固め

何を指摘の柱とするかで苦労した。書いてみてはメンバーで討議し、また書き直すループを3回ほど繰り返した。何故、ウォーターフォール方式に進行しなかったのであろうか。反省するに、骨子を決める会合に参加できなかった事実がある。報告を作る最初の時点で私と他のメンバーとの間でベクトルが狂ってしまったようだ。従ってしっくりしないまま試行錯誤をしたようだ。

次回にはベクトル合わせを徹底的に議論したい。さらにベクトル合わせを前倒しすべきと考える。少なくとも本調査に入る前、できれば資料を見た後、予備調査に入る前に一晩徹夜するつもりで話し合ってみたい。このような前倒しにより、報告書作成時点で顕在化した、質問の網羅性、質問の深さに関する弱点も予防できるのではなかろうか。

2. ワークロード

78.5時間が監査に費やした時間の合計である。かなりの時間を使ったものである。初めてのチャレンジであること、断続的作業でオーバーヘッドが増えることを差し引いても少々かかり過ぎと思う。ビジネスとして行うならば、1/3か1/4にしなければペイしないであろう。

もし、費用を請求するとしたら、時間単価1万円として、約80万円の請求になる。もっとも対価を払う人がいるとしての話だが。

全工数のかなりの部分を就業時間内に行ったが、スキルアップのためとはいえ、認めてくれた会社に感謝している。

3. リードタイム

1月14日の社長インタビューからスタートし、5月11日に報告会を行って、監査の全工程を完了させた。約4ケ月のリードタイムを要している。正直言って長すぎると感じる。スタートして気分が盛り上がってきたが、時間の経過と共に何度か面倒くさくなってきた時期があった。同様に被監査側も途中で気が抜けてしまったのではなかろうか。また、時間がたち過ぎてしまい、監査報告書をうけても、ありがたみも薄れてしまったのではないかと危惧する。

緊張感を持ち続けるには短期間に一気に仕事を片づけてしまうのに限るので、次回にはリードタイムを半減させたい。監査者は全員本業外で従事しているが、もう少し従業帯を凝縮させることは可能と思う。

4. リーダー交代

当社のリーダーが長期出張を命じられ、監査に参加できなくなる事態が生じた。7人のメンバー中、私を含め4人が仮免の教習生であるグループのリーダーが居なくなってしまい、この先どうなるものかと心配したが、吉田さんがリーダー役をかって出てくださり、無事に航海を続けることができた。正に、things happenであるが、ものごと何とかなる、もまた真実であった。何だか自身の人生を垣間見たようである。

Y社システム監査を体験して

No.766 ビック東海 遠山 貴志

昨年12月より事例研究会で実施していた、Y社のシステム監査が5月11日の報告会を以て終了しました。期間にして5ケ月弱、私個人の所要工数は0.7人月弱と、予想したより長い期間と少ない工数(メンバーの中では多かったようですが)で終わることができました。途中、仕事の都合でリーダーが替わるという事態も発生しましたが、吉田さん、松枝さんの的確な指導と鈴木座長を始めとする皆さんのアドバイスにより無事、完了することができました。

私自身の監査の経験は、昨年11月に開催されたSAAJシステム監査実践セミナーを受講した後、社内の電算センターの監査をしただけで、社外の監査を、しかも事例研のメンバー(当たり前ですがいろいろな会社の人!)とタスクフォース的に作業をするというのは未知の領域のことで非常に勉強になりました。例えばヒアリングの際、事実を正しく捉え、その内容について思い込みを排除してまとめること、そしてその為の有効なヒアリング項目抽出の必要性。或いは個々の問題に固執せず、全体を俯瞰していく事の大切さ。また、実践セミナーでも教えられましたが、監査対象企業レベルを考慮して物事を考える姿勢については報告書をまとめる上でも役に立ちました。特に、Y社ではシステムの移行が必須で、どうするべきかは分かっていましたが、どのようにすべきかはトップの意思、情報化投資への考え、現場のモチベーション等が絡んで来ます。あるべき姿は分かっていても、経過としてどのようにすべきか、或いはどのような選択肢があるかを提示し、相手に選ぶ猶予を与えること。これは監査の有効性を高める為にも重要なことだと感じました。

今回の監査チームの中では、森本さん、桜井さん、私の３人が昨年の実践セミナーの受講者で、三輪さんも風邪で欠席したものの申し込みをしており、ニューフェイスが多かった訳ですが、皆さん本業との狭間で時間をやりくりしながら真摯に取り組んでおられました。また、小坂さんも含めメンバー全員での打合せにおいては、監査の有用性の観点から議論になることもありましたが、今となっては妙になつかしい気がします。

とはいっても、これは今後も重要なテーマであり、その重要性を知識としてだけではなく、体験として獲得できたという事は一番の成果だったのではないかと思います。今はしばらくゆっくりしていたい気分ですが、また、機会があればトライしてみたいと思います。その節はまたよろしくお願いいたします。

セキュリティ研究会活動報告

No.25 金子 長男

・通産省 情報処理振興課訪問

４月27日に通産省情報処理振興課安全指導係、澤野係長を訪問し、セキュリティ研究会の成果物である診断支援ソフト(安全対策診断支援ソフト、情報システム大震災対策調査支援ソフト)のご紹介をさせていただきました。澤野係長にはお忙しいところ時間を取っていただきありがとうございました。本誌において御礼申し上げます。

訪問者は橘和会長、木村理事、岩崎理事及び金子の４名です。

総会(２月27日)の懇親会の場で澤野係長に口頭でツールの説明はしました。しかし、実際に見て感想をいただきたい、協会ではこのような活動も行っていることを知っていただきたい、何かの際に話題にしていただけたならば、等の理由で今回のご訪問となりました。

ノート型パソコンを持ち込み、昨年会員に配付したソフトを使ってデモを行いました。

ソフトの評価は上々だったと思います。デモの後、ソフトについて論議を行いました。意見としては、システム監査の支援ソフトとしては十分役立つのではないか、各企業で自社向けにカスタマイズしても使えるため使用の範囲が広がるのではないか、など意見がでました。しかし、やはり重要なことは実施例を多く収集する事であり、協会会員企業を手始めにまず使ってもらい、評価をいただくことがこれからの取り組みとして重要であるという認識は全員一致したようです。

約１時間程のデモでしたが、我々の訪問主旨は十分達成したと思います。

会員各位へのお願い

自社で「安全対策診断支援ソフト」または「情報システム大震災調査支援ソフト」を使用した方は、ぜひ評価をいただきたい。

また、まだ使用していない方は是非、自社で診断をお願いいたします。そして、評価を研究会までお寄せ下さい。

会員が一部執筆した書籍のお知らせ

協会顧問(元事務局長)で(株)ケンウッド情報システム部長の鈴木信夫氏(会員No.8)が、このほど出版された「ERP導入マネジメント」(監修編者：ERP研究推進フォーラム、発行：情報処理振興事業協会(IPA)／(株)アイネス)のうち、第3章ERP導入の先進事例に学ぶー11社の中の1社として執筆されているので、ご紹介します。

同書は、ERP研究推進フォーラムが総力を結集して、来るべきERP本格化時代を前に、ユーザ企業の経営者や導入プロジェクトリーダに、ベンダやSI企業に偏らない情報を提供しようというものです。

構成は、B5版、440ページ(定価3990円)で、

第1章　今なぜERPか
第2章　ERPとは何か
第3章　導入事例
第4章　導入のために経営者は何をなすべきか
第5章　同じくプロジェクトリーダは何をなすべきか

となっており、特に第4章、第5章では240ページを当てて、ユーザ側がベンダやSI企業に主体的に立ち向かえるようなマニュアルを目指しており、第3章の事例の充実度も注目されています。

企画意図や内容の濃さで欧米にも例がなく、日本でも初めての本格版といえましょう。補助金を出したIPAでも、「地域ソフトウェアセンター」等での教科書として使います。

(株)アイネスの関わりは、ERPフォーラムが任意団体でIPAとの契約などで締結能力がなく、その代行および今後の普及への支援だそうです。

ERPを主要業務にされる所はもちろん、少しでも関心のある向きには、お目通しをお勧めします。

新システム監査基準実務手順書'98 同封ＦＤ取扱い説明書

SAAJ新システム監査基準プロジェクト

1．本FDの構成

A：¥KIJUN98(監査基準実務手順書のテキスト形式ファイルのディレクトリ)
¥KIJNEXCL.EXE(監査基準実務手順書のEXCEL95の形式ファイル自己解凍書)
¥HAJIME I .TXT(はじめに)
¥HYOSI.TXT(表紙)
¥MOKUJI.TXT(目次)
¥README.TXT(取扱い説明書)→最初に開いて読んでください！
¥RENRAKU.TXT (連絡先)

2．EXCEL95ファイルの解凍処理

(1) FD全体をハードディスク上にコピーして下さい。
(2) エクスプローラ上で「KIJNEXCL.EXE」を、ダブリルクリックすると自己解凍処理

が開始されます。

解凍先ディレクトリの既定値は「C：¥」となっていますので、任意に変更してください。

解凍処理実行後指定したディレクトリに、EXCEL95形式ファイルが入った「KIJUN98」のディレクトリが作成されます。

新規入会個人会員

番号	氏名	勤務先・所属	
806	諸藤 雅之	エフコープ生活共同組合	内部監査
807	浦上 豊蔵	三洋電機(株)	CEメディア事業本部本部室
808	若原 達郎	東邦ガス(株)	情報システム部
809	角野 晃之	国際コンピュータシステム(株)	システム開発部金属システム研究グループ
810	岡田 博基	東邦ガス(株)	情報システム部
811	船津 宏	九州日本電気ソフトウエア(株)	第一応用システム事業部
812	島本 栄光	第二電電(株)	情報システム部
813	遠藤 俊郎	(株)NHKコンピューターサービス	運用第三部
814	高田 健一	静岡産業技術専門学校	
815	剣持 訓司	大興電子通信(株)	SIビジネス統括部
816	鈴木 昌治	監査法人トーマツ	東京事務所トータルサービス
817	達 靖志	ジェーアール東日本情報システム	
818	田端 稔雄	(財)大阪港開発技術協会	工務部
819	永井 孝一	日本出版販売(株)	システム部
820	落合 崇成	ウッドランド(株)	エルム事業部
821	楠 正彦	長銀システム開発(株)	システム部
822	田中 勝弘	(株)コンピュータ・テクノロジー・インテグレイタ	SI事業部
823	長倉 宇一郎	コベルコシステム(株)	ソリューションシステム本部システムセンター
824	西崎 傳生	シュルンベルジェ(株)	スマートカード事業部
825	唐沢 鉄夫	中央クーパース&ライブランド・コンサルティング	
826	松野 祐治	(株)三菱総合研究所	先進科学部
827	古賀 秀敏	明生システムサービス(株)	総合システム事業部第一P開発室

新規入会法人会員

6015	森末 清成	日本インフォメーション・エンジニアリング(株)	西日本支社ITコンサルティング部

発行所 日本システム監査人協会
発行人 橘和 尚道
事務局 〒151 東京都渋谷区笹塚2－1－6
笹塚センタービル5F
(株)産能コンサルティング内
TEL. 03(5350)9268 FAX. 03(5350)9269
ホームページ http://www.saaj.or.jp/
※ご連絡はなるべく郵便または、FAXでお願いします

会報担当(ご投稿、ご意見、ご要望は下記まで)
三谷慶一郎 (株)NTTデータ経営研究所
TEL. 03(5467)6321 FAX. 03(5467)6322
QZG07732@niftyserve.or.jp
金子 長男 (財)公営事業電子計算センター
TEL. 03(3343)4560 FAX. 03(3343)6742
kaneko@pvc.or.jp
富山 伸夫 (株)データ総研
TEL. 03(5695)1651 FAX. 03(5695)1656
GFF00037@niftyserve.or.jp
片寄早百合 日本NCR(株)
TEL. 03(5456)6156 FAX. 03(5456)6436
Sayuri.katayose@Japan.NCR.COM
吉田 裕孝 三井物産(株)
TEL. 03(3285)2058 FAX. 03(3285)9939
Hi.Yoshida@xm.mitsui.co.jp